



TSA Registered Traveler

Appendix E:
Sample System Security Plan Template

Version 3.0, May 2007



Transportation
Security
Administration



Appendix E: Sample System Security Plan Template

The following sample has been provided ONLY as one example based on NIST SP 800-18 Revision 1 — Guide for Developing Security Plans for Federal Systems. Service Providers may be using other formats and choose to update those to reflect any existing omissions based on this guidance. This is not a mandatory format; it is recognized that Service Providers may have developed and implemented various approaches for information system security plan development and presentation to suit their own needs for flexibility.

Information System Security Plan

1. Information System Name/Title:

[Unique identifier and name given to the system.]

2. Information System Categorization:

[Identify the FIPS 199 categorization.]

3. Information System Owner:

[Name, title, department, address, email address, and phone number of person who owns the system.]

4. Authorizing Sr. Management:

[Name, title, department, address, email address, and phone number of the senior management official designated as the authorizing official.]

5. Other Designated Contacts:

[List other key personnel, if applicable; include their title, address, email address, and phone number.]

6. Assignment of Security Responsibility:

[Name, title, address, email address, and phone number of person who is responsible for the security of the system.]

7. Information System Operational Status:

[Indicate the operational status of the system. If more than one status is indicated, list which part of the system is covered under each status.]

8. Information System Type:

[Indicate if the system is a major application or a general support system. If the system contains minor applications, list them in Section 9. General System Description/Purpose.]

9. General System Description/Purpose

[Describe the function or purpose of the system and the information processes.]

10. System Environment

[Provide a general description of the technical system. Include the primary hardware, software, and communications equipment.]

11. System Interconnections/Information Sharing

[List interconnected systems and system identifiers (if appropriate), provide the system, name, organization, system type (major application or general support system), indicate if there is an ISA/MOU/MOA on file, date of agreement to interconnect, FIPS 199 category, and the name of the authorizing official.]

System Name	Organization	Type	Agreement (ISA/MOU/MOA)	Date	FIPS 199 Category	Auth. Official
-------------	--------------	------	-------------------------	------	-------------------	----------------

12. Related Laws/Regulations/Policies

[List any laws or regulations that establish specific requirements for the confidentiality, integrity, or availability of the data in the system.]

13. Minimum Security Controls

[Provide a description of how the TSA-recommended security controls are being implemented or planned to be implemented. The description shall contain: 1) the security control title; 2) how the security control is being implemented or planned to be implemented; 3) any scoping guidance that has been applied and what type of consideration; and 4) indicate if the security control is a common control and who is responsible for its implementation.]

14. Information System Security Plan Completion Date: _____

15. Information System Security Plan Approval Date: _____

National Institute of Standards and Technology. (2006). *Special Publication 800-53: Recommended Security Controls for Federal Information Systems*. Gaithersburg, MD: A. Johnson, S. Katze, A. Lee, G. Rogers, R. Ross, M. Swanson, G. Stoneburner.